RESEAU-CANOPE.FR

CANOPÉ

RÉSEAU DE FORMATION DES ENSEIGNANTS

CHARTE DE BON USAGE

DES MOYENS NUMERIQUES

ET DES SYSTEMES D'INFORMATION DE RESEAU CANOPE

Table des matières

1. Préambule 5
2. Champ d'application 5
2.1. Entrée en vigueur de la Charte 5
2.2. Diffusion 5
2.3. Modalité d'application de la Charte 5
3. Objectifs 6
4. Règles générales d'utilisation et de bon usage 6
4.1. Respect des lois, des réglementations et de la déontologie 6
4.2. Protection des ressources sous la responsabilité de l'utilisateur/utilisatrice 6
4.2.1. Responsabilité de l'utilisateur/utilisatrice 7
4.2.2. Responsabilités des services support des SI 7
4.3. Connexion 7
4.3.1. Accès depuis des locaux de Réseau Canopé 7
4.3.2. Télétravail et nomadisme 8
4.4. Protection des données 8
4.4.1. Accès 8
4.4.2. Comptes des agents et mot de passe 8
4.5. Continuité de service 8
4.6. Internet 9
4.6.1. Utilisation 9
4.6.2. Visio et audio conférences 9
4.7. Messagerie électronique 9
4.7.1. Règles générales 9
4.8. Utilisation de Smartphones personnels pour l'accès à la messagerie professionnelle. 10
4.9. Utilisation des imprimantes multifonctions (scanner-fax) 10

4.10. Impressions de documents confidentiels 10
4.11. Utilisation des ressources à des fins privées 11
4.12. Utilisation des ressources par les organisations syndicales 11
4.13. Données professionnelles 11
4.14. Départ de l'agent 11
5. Contrôle des activités 12
5.1. Contrôles automatisés 12
5.2. Contrôle de l'utilisation des ressources 12
6. Signalement d'incidents 12
7. Sanctions 13
1. Les textes généraux 14
2. Textes et dispositions spécifiques : 14
2.1. Protection des données à caractère personnel 14
2.1.1. Niveau national 14
2.1.2. Niveau européen 14
2.2. Propriété intellectuelle 14
3. Les textes répressifs 15
3.1. Dispositions du code pénal 15
3.2. *(Extraits)* Dispositions pénales du code de la propriété intellectuelle 16
Glossaire

Charte de bon usage des moyens numériques et du SI

1. Préambule

La présente Charte a pour objet de définir les règles d'accès et d'usage des moyens numériques et du système d'information (SI) de Réseau Canopé.
Elle a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'établissement et fait de l'utilisateur/utilisatrice un acteur essentiel à la réalisation de cet objectif.
Elle permet d'informer l'utilisateur/utilisatrice sur :

- les usages autorisés des moyens numériques mis à sa disposition ;
- les règles de sécurité en vigueur ;
- les mesures de contrôle prises par l'établissement ;
- et les sanctions encourues par l'utilisateur/utilisatrice.

Le bon fonctionnement du SI repose sur le respect des dispositions législatives et réglementaires. Le « bon usage » des ressources numériques et des SI fait l'objet **d'un guide de bonnes pratiques et de mise en œuvre** de la présente charte. Ce guide est un document pratique et autonome. L'utilisateur/utilisatrice est invité(e) à le consulter sur l'intranet de l'établissement

2. Champ d'application

La présente charte s'applique à l'ensemble des personnels participant à quelque titre que ce soit à la mission du Réseau Canopé, dès lors qu'ils sont sous l'autorité de son directeur général, ainsi qu'au personnel des sociétés prestataires, des partenaires externes et leurs sous-traitants accédant au SI de Réseau Canopé.
Les entités chargées des relations contractuelles et opérationnelles avec ces prestataires ou partenaires, doivent donc s'assurer du respect de la charte sur le périmètre d'actions impactant le Système d'Information.

Les moyens numériques représentent l'ensemble des données, des logiciels et des matériels, des outils informatiques et des services numériques que Réseau Canopé met à disposition de ses utilisateurs/utilisatrices.

2.1. Entrée en vigueur de la Charte

La présente Charte actualisée a été soumise pour avis au comité social d'administration du 18/11/2025 et est applicable immédiatement.

2.2. Diffusion

La Charte est annexée au règlement intérieur de l'établissement.
La Charte est disponible sur l'intranet.

La présente charte est également communiquée à chaque agent à son arrivée dans l'établissement par un mail automatisé.

La charte sera annexée aux marchés publics dont l'exécution implique l'accès aux ressources.
Tout contrat passé entre Réseau Canopé et un tiers impliquant l'accès de ce tiers aux ressources numériques et aux SI stipule que le contractant s'engage à faire respecter la présente Charte par son propre personnel et, le cas échéant, par ses sous-traitants.

2.3. Modalité d'application de la Charte

La Direction Générale est chargée de l'exécution de la Charte.
La DSI et le Responsable Sécurité des Systèmes d'Information (RSSI) mettent en place toutes les mesures techniques nécessaires à son application et au contrôle de son exécution.
L'ensemble des managers de l'établissement veillent au respect de la Charte au sein de l'entité dont ils sont responsables.

3. Objectifs

La présente Charte a pour objet de :

- Maintenir la confidentialité, l'intégrité et la disponibilité du SI
- Maintenir la qualité de service du SI à son meilleur niveau
- Préciser la responsabilité des différents utilisateurs/utilisatrices
- Respecter la sécurité du SI
- Participer activement au bon fonctionnement du SI
- Servir de document de référence concernant les usages des moyens numériques et des SI

4. Règles générales d'utilisation et de bon usage

4.1. Respect des lois, des réglementations et de la déontologie

Les utilisateurs/utilisatrices sont soumis au secret professionnel ou à l'obligation de discrétion professionnelle et veillent au respect de la confidentialité des informations en leur possession.
Ils doivent veiller au respect des droits de propriété intellectuelle, au secret des correspondances, à la confidentialité des données personnelles, et au droit à l'image.

Il est notamment interdit :

- De publier tout propos contraire à la loi (notamment la diffamation, l'injure, les incitations aux crimes, à la discrimination, à la haine notamment raciale, le révisionnisme et l'apologie des crimes, la compromission de mineurs ou leur exposition à des messages à caractère violent ou pornographique, ou toute incitation à la consommation de substances interdites), aux règles d'éthique et de déontologie,
- De porter atteinte à la vie privée d'autrui (sujets relatifs entre autres aux opinions politiques, philosophiques ou religieuses, aux origines ethniques, à l'orientation sexuelle ou à la santé des personnes),
- De diffuser ou de télécharger des informations protégées par le droit d'auteur qu'il s'agisse notamment d'écrits, d'images, de logiciels ou de bases de données, et de porter atteinte à tout signe distinctif appartenant à des tiers, en particulier aux droits de marques, nom commercial et nom de domaine,
- De commettre tout acte relevant de la fraude informatique : falsification, modification, suppression ou introduction d'informations avec l'intention de nuire.

4.2. Respect du Règlement Général sur la Protection des Données et de la loi informatique et libertés

Tout utilisateur doit se conformer au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le RGPD (Règlement Général sur la Protection des Données) et à la loi du 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par l'ordonnance du 12 décembre 2018.

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent. Toutes les créations de fichiers comprenant ce type d'informations, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi Informatique et Libertés. En conséquence, tout utilisateur souhaitant procéder à un tel traitement devra

effectuer une déclaration de traitement de données à caractère personnelle auprès du Délégué à la Protection des Données à l'adresse dpo@reseau-canope.fr

Par ailleurs, conformément aux dispositions prévues par le RGPD et Loi Informatique et Libertés, chaque utilisateur dispose d'un droit d'accès, de rectification et de limitation au traitement de ses données personnelles, y compris les données portant sur l'utilisation des systèmes d'information. Ce droit s'exerce auprès du délégué à la protection des données de l'établissement.

4.3. Protection des ressources sous la responsabilité de l'utilisateur/utilisatrice

4.3.1. Responsabilité de l'utilisateur/utilisatrice

L'utilisateur/utilisatrice est responsable des équipements et contenus qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il/elle doit concourir à la protection desdites ressources en faisant preuve de vigilance et de prudence. Ainsi il/elle ne doit pas transmettre d'informations professionnelles à des tiers, lesquelles ne seraient pas strictement nécessaires à l'accomplissement des missions confiées, sauf accord express de son/sa supérieur(e) hiérarchique.

L'utilisateur/utilisatrice peut se rapprocher du/de la DPO pour toutes questions relatives aux données personnelles.

L'utilisateur/utilisatrice standard n'a pas les droits d'administration de son poste de travail (PC agent) et ne peut installer de logiciel sans recourir aux services support.
Les postes de travail dans les Ateliers Canopé destinés aux usagers (pour les formations, médiations) ont un statut particulier permettant aux formateurs de réaliser un certain nombre d'actions qui seront formalisées dans le cadre d'une charte des administrateurs telle que définie dans l'article ci-dessous.

4.3.2. Responsabilités des services support des SI

Sont considérés comme services support des SI les équipes qui assistent les utilisateurs/utilisatrices dans l'utilisation des outils numériques (dépannage technique sur les postes, accompagnement à la saisie dans les outils métiers, administrateurs techniques ou fonctionnels).
Compte tenu des droits étendus dont ils disposent, ces équipes portent une responsabilité plus grande dans la sécurité des systèmes d'information.
Les utilisateurs/utilisatrices ayant des fonctions d'administrateur des moyens numériques sont soumis à la charte des administrateurs des SI précisant leurs obligations particulières.

4.4. Connexion

4.4.1. Accès depuis des locaux de Réseau Canopé

Depuis les locaux du Réseau Canopé,

- **l'accès à Internet à partir d'un matériel professionnel est uniquement autorisé au travers des infrastructures configurées et fournies par la DSI (Réseau filaire ou Wifi Canopé).**

- **l'accès au réseau local est uniquement autorisé à partir d'un matériel professionnel fourni et géré par Canopé.**

Il est par conséquent strictement interdit, de connecter des matériels numériques (personnel ou professionnel) simultanément au réseau de Canopé et à un réseau tiers (wifi ou VPN) pour des raisons de sécurité.

Il est interdit aux utilisateurs/utilisatrices d'installer tout équipement partageant une connexion réseau (borne wifi par exemple).

Le matériel non professionnel peut être connecté à Internet au travers du réseau wifi invité.

4.4.2. Télétravail et nomadisme

Les accès distants aux applications sensibles sont uniquement autorisés par le biais des systèmes de communication sécurisés (VPN) mis en place par l'équipe chargée de la gestion centralisée des réseaux informatiques (cf annexe du protocole du télétravail). L'utilisateur/utilisatrice ne cherchera pas à accéder à distance aux ressources informatiques par tout autre moyen.

Dans le cas du nomadisme et des accès Internet public (trains, hôtels...), il est obligatoire d'utiliser le VPN pour garantir la sécurité de la connexion. Un lancement automatique du VPN est à l'étude par la DSI.

La plus grande vigilance est nécessaire de la part des utilisateurs/utilisatrices d**ans le cadre de l'accès à Office 365** et dans le cadre de l'usage de cet outil. Il est déconseillé d'utiliser cet outil sur un matériel non professionnel. Il est prévu le déploiement généralisé du MFA (authentification multi facteurs) à l'ensemble des utilisateurs durant l'année 2025. Cette nouvelle mesure de sécurité est rendue obligatoire par la DSI.

L'utilisateur/utilisatrice veillera à garantir la sécurité du matériel d'accès utilisé et il protégera les données qu'il contient.

4.5. Protection et confidentialité des données de Réseau Canopé

4.5.1. Accès

L'utilisateur/utilisatrice ne doit pas chercher à accéder à des données ou à des ressources pour lesquelles il n'est pas dûment autorisé et habilité.
Il est informé des règles d'utilisation (accès, traitement, stockage…) et doit respecter les règles de communication des informations pouvant exister au sein de son organisation.

4.5.2. Comptes des agents et mot de passe

Les comptes d'accès au SI sont personnels et confidentiels.
Les droits d'accès à tout ou partie du SI reposent sur ce compte d'accès.

Les mots de passe fournis par défaut par la DSI, par les éditeurs ou les fabricants sont à remplacer immédiatement.

4.6. Continuité de service

Les informations professionnelles nécessaires à la continuité des activités doivent être stockées sur des espaces collaboratifs fournis par Réseau Canopé.
L'utilisateur/utilisatrice est responsable des informations et doit veiller à en préserver la confidentialité et ne les partager qu'avec les personnes habilitées à y accéder.

Les documents professionnels doivent obligatoirement être stockés dans des espaces synchronisés avec OneDrive afin de garantir la sauvegarde automatique et sécurisée des données de l'établissement. Cette méthode permet de minimiser les risques de perte d'informations, notamment en cas de défaillance ou de vol du matériel numérique professionnel.

L'utilisateur/utilisatrice ne doit jamais supprimer ou modifier, de sa propre initiative, des informations pouvant être nécessaires au bon déroulement des activités de Réseau Canopé.
Il ne doit pas stocker de documents professionnels sur du matériel personnel.

4.7. Internet

4.7.1. Utilisation

Dans le cadre de ses activités, tout agent a accès à Internet.

La consultation de sites Internet ou le téléchargement de fichiers qui pourraient être considérés comme illégaux sont interdits.

Pour des raisons de sécurité ou sur décision, l'accès à certains sites peut être limité ou prohibé par le RSSI.
Celui-ci est habilité à imposer des configurations du navigateur et à bloquer le téléchargement de certains fichiers.

4.7.2. Visioconférences

Les outils de visioconférences mis à disposition par la DSI ou le ministère de tutelle sont à utiliser lors de communication interne Canopé et recommandés en priorité pour les partenaires extérieurs.
L'utilisation de tout autre outil sera soumise à des tests préalables et pourra donner lieu à une validation et à une intervention du support SI.

4.8. Messagerie électronique

4.8.1. Règles générales

L'attention des utilisateurs/utilisatrices est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et qu'il peut, de plus, être rapidement communiqué à des tiers.
L'utilisateur/utilisatrice doit veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tels que des propos diffamatoires, injurieux ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

L'utilisateur/utilisatrice est responsable du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie professionnelle, étant précisé que le/la supérieur(e) hiérarchique dispose d'un droit d'accès à ses messages, sauf dans le cas où l'objet du message précise clairement son caractère personnel.

Avant tout envoi, il est impératif de vérifier l'identité et l'habilitation des destinataires du message devant recevoir les informations transmises.

L'utilisateur/utilisatrice doit informer l'émetteur d'un message électronique qui ne lui est pas destiné. Il doit veiller à effacer ce message de son ordinateur et, dans la mesure du possible, ne pas le lire.

Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

Afin d'éviter tout risque de corruption du SI, l'agent ne doit jamais sauvegarder ou ouvrir des pièces jointes suspectes.

Afin d'éviter la problématique liée aux courriers indésirables, il est demandé à chaque utilisateur/utilisatrice de ne jamais diffuser son adresse professionnelle sur des sites non professionnels.

Aucune réponse ne doit être apportée aux messages électroniques externes demandant des informations personnelles.

De manière générale, les informations confidentielles ou sensibles doivent être échangées en toute sécurité.
Ainsi :

- Le transfert de ce type d'informations vers des messageries n'appartenant pas au réseau professionnel de l'agent est strictement interdit.
- La redirection automatique de toute boîte aux lettres électronique vers la boîte aux lettres professionnelle de Réseau Canopé est prohibée.

Les informations sensibles ne doivent jamais être échangées au travers des messageries instantanées professionnelles ou non professionnelles qui ne garantissent pas l'identité du destinataire.

4.9. Utilisation de Smartphones personnels pour l'accès à la messagerie professionnelle.

L'accès à la messagerie professionnelle à partir d'un smartphone personnel n'est pas autorisé si le compte utilisateur ne dispose pas de mesures de sécurité minimales. L'authentification multifacteurs (MFA) est obligatoire pour y accéder.
L'utilisateur/utilisatrice est particulièrement responsable de la protection des messages ou pièces jointes récupérées et stockées sur ce type de périphérique. Il veillera à en limiter l'accès par une protection adéquate (chiffrement, code de verrouillage).
Il signalera toute perte et vol à la DSI.

4.10. Utilisation des imprimantes multifonctions (scanner-fax)

L'envoi d'informations par télécopieur peut comporter des risques car l'identité de la personne qui réceptionnera le document ne peut être garantie.
L'utilisation de ces appareils est déconseillée pour des informations sensibles.
Les accusés d'envoi/réception, contenant souvent une copie des éléments transmis, ne doivent pas être laissés sur les télécopieurs.

4.11. Impressions de documents confidentiels

Les documents confidentiels, contenant des informations personnelles ou des informations sensibles doivent être récupérés rapidement et ne pas rester sur l'imprimante.
Il est recommandé d'utiliser un code pour déclencher l'impression des documents confidentiels.

4.12. Utilisation des ressources à des fins privées

Les ressources informatiques mises à la disposition des utilisateurs/utilisatrices sont destinées à un usage professionnel. Un usage personnel raisonnable est toléré sous réserve qu'il n'entre pas en conflit avec l'usage professionnel ni le bon fonctionnement du SI.

Concernant Internet, l'utilisateur/utilisatrice ne devra pas nuire à la qualité du débit en consultant des sites consommateurs de bande passante (Vidéos, télévisions, radios …)

Les messages à caractère personnel sont tolérés.

4.13. Utilisation des ressources par les organisations syndicales

Les messages à caractère syndical sont soumis à des dispositions particulières. Seules les organisations syndicales ont la possibilité de diffuser une information syndicale. Les organisations syndicales feront particulièrement attention à réduire la taille des mails lors des envois en masse, en privilégiant par exemple le renvoi vers des liens Internet ou Intranet plutôt que des pièces jointes. Les dispositifs d'accès aux technologies de l'information et de la communication (TIC) au profit des organisations syndicales ont été mis en œuvre à Réseau Canopé (cf. Note du 18/01/2018) et respectent la décision ministérielle du 26/04/2016 relative aux conditions et aux modalités d'utilisation des TIC.

Les messageries, les agendas et les dossiers des représentants du personnel sont considérés comme privés.

4.14. Données professionnelles

En l'absence d'indication contraire, toute information est considérée par défaut comme étant professionnelle et appartenant à Réseau Canopé.

Si l'espace d'un disque est saturé par des données personnelles, l'utilisateur/utilisatrice devra supprimer ces données.

L'utilisateur/utilisatrice est entièrement responsable de la gestion de ses données personnelles.
L'utilisateur/utilisatrice ne pourra tenir pour responsable Réseau Canopé des incidents survenant à ces données personnelles (perte de fichiers suite à une panne matérielle par exemple, ou suppression suite à une infection virale).

4.15. Départ de l'agent

En cas de départ, l'agent est informé de la date de clôture de son compte et il lui appartient de récupérer puis supprimer ses données personnelles (y compris celles de messagerie). Il veille à ne pas supprimer d'informations professionnelles lors de ces opérations.

Lors d'un départ définitif ou d'une absence ponctuelle, l'utilisateur/utilisatrice informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.

Le compte de l'utilisateur/utilisatrice partant est désactivé et le contenu professionnel de la boîte de messagerie sera conservé pour une période maximale d'un mois. L'utilisateur/utilisatrice est le/la seul(e) habilité(e) à pouvoir assurer le transfert d'informations professionnelles avant son départ effectif pour assurer la continuité de service.

L'utilisateur/utilisatrice a obligation de restituer tous les matériels informatiques à Réseau Canopé.

5. Contrôle des activités

5.1. Contrôles automatisés

Les agents sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication.

L'attention des agents est attirée sur le fait que des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Ainsi, la DSI est amenée, entre autres, à surveiller et à analyser (de manière globale et non individuelle) :

- L'utilisation d'Internet,
- L'utilisation de la messagerie électronique,
- L'utilisation des téléphones et télécopieurs,
- L'utilisation des imprimantes
- L'accès aux postes de travail et aux applications ainsi que les actions effectuées,
- Les accès aux répertoires partagés ou aux outils collaboratifs.

Ces traces techniques sont conservées pour une période maximale d'un an.
Cette surveillance s'exerce dans le respect des droits des agents conformément aux dispositions de la loi du 6 janvier 1978 modifiée et des dispositions du code des postes et des communications électroniques.

5.2. Contrôle de l'utilisation des ressources

Dans le cadre de sa maîtrise de l'allocation des ressources et de sa politique de sécurité du réseau, la DSI se réserve le droit de poser des limites à l'utilisation d'Internet ou de la messagerie tels que la mise en place de dispositifs de filtrage de sites non autorisés ou l'interdiction de téléchargement ou de connexion.

Des outils de contrôle de la messagerie tels que les outils de détection de virus ou filtres anti-spam sont mis en œuvre.

Aucun traitement généralisé n'est effectué pour contrôler de manière systématique l'activité individuelle des agents.

Un usage anormal des moyens numériques mis à disposition, et contraire aux règles posées par la présente charte, sera susceptible d'entraîner des poursuites disciplinaires en application des règles qui les régissent.

6. Signalement d'incidents

Toute anomalie suspectée ou avérée concernant le SI de Réseau Canopé (vols ou pertes de matériel, vols ou pertes d'Informations, dysfonctionnements du poste de travail, incident sur une application), ou toute violation des règles décrites dans la présente charte**, doit être signalée au support SI et au responsable hiérarchique, qui traiteront l'incident.**

Concernant les cas plus spécifiques d'atteinte à la sécurité du SI et de fuite de données personnelles, **le RSSI (rssi@reseau-canope.fr) et le DPO - délégué à la protection des données - (dpo@reseau-canope.fr) doivent être informés sans délai.**

7. Sanctions

En cas de violation des dispositions de la présente charte, Réseau Canopé se réserve le droit de diligenter des procédures disciplinaires à l'encontre de leurs auteurs conformément aux textes en vigueur, sans préjudices d'éventuelles sanctions judiciaires.

Par ailleurs, Réseau Canopé pourra procéder à la suspension des droits d'accès de l'agent au SI.

Concernant les utilisateurs/utilisatrices liés par un contrat de prestation ou une convention, tels que les étudiants en stage, les partenaires ou les fournisseurs, toute violation des règles édictées par la présente charte, hors cadre dérogatoire, peut entraîner la rupture dudit contrat voire des poursuites judiciaires à l'égard de l'entreprise d'origine ou de la personne concernée.

En cas de doute sur la légalité d'une opération, les agents peuvent consulter le code de la propriété intellectuelle sur le site Internet www.legifrance.gouv.fr. Pour tout conseil pour l'application de la présente charte, il est possible de s'adresser au RSSI de Réseau Canopé.

Cas d'un prestataire ou personnel externe à Canopé

Nom, Prénom et fonction de la personne concernée

……

……

Intitulé du projet, du marché ou de la convention nécessitant l'accès au SI de Canopé

……

……..

Date de début et de fin du projet, du marché ou de la convention

Date début : …/…/…

Date fin : …/…/….

Je déclare avoir pris connaissance du contenu de cette charte et m'engage à respecter les règles édictées

Signature de la personne concernée

Annexe : Principaux textes juridiques

1. Les textes généraux

- **Loi n°83-634 du 13 juillet 1983** portant droits et obligations des fonctionnaires
- **Loi n°84-16 du 11 janvier 1984** relative à la fonction publique de l'État
- **Décret n°84-961 du 25 octobre 1984** relatif à la procédure disciplinaire concernant les fonctionnaires de l'État
- **Décret n°94-874 du 7 octobre 1994** fixant les dispositions communes applicables aux stagiaires de l'État
- **Décret n°86-83 du 17 janvier 1986** aux dispositions générales applicables aux agents contractuels

2. Textes et dispositions spécifiques :

2.1. Protection des données à caractère personnel

2.1.1. Niveau national

- **Loi n°78-17 du 6 janvier 1978 dite loi « Informatique et Libertés »** modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

2.1.2. Niveau européen

- **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016** relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- **Convention du 28 janvier 1981 du Conseil de l'Europe** pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
- **Directive européenne 95/46 du 24 octobre 1995**, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- **Directive européenne 97/66 du 15 décembre 1997** concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

Toute personne ou service, souhaitant mettre en œuvre un traitement de données à caractère personnel doit se rapprocher au préalable du Délégué à la Protection des Données (dpd@reseau-canope.fr)

2.2. Propriété intellectuelle

- **Article L122-6 du Code de la propriété intellectuelle :** Sous réserve des dispositions de l'article L. 122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :
    - 1° La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;

- 2° La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;
- 3° La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un État membre de la Communauté européenne ou d'un État partie à l'accord sur l'Espace économique européen par l'auteur ou avec son consentement épuise le droit de mise sur le marché de cet exemplaire dans tous les États membres à l'exception du droit d'autoriser la location ultérieure d'un exemplaire.

3. Les textes répressifs

À titre d'exemple, ci-dessous une liste de dispositions légales exposant les peines maximales sanctionnant des infractions liées à l'usage des moyens informatiques

3.1. Dispositions du code pénal

- **Article 226-16 du Code Pénal** : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
- **Article 226-17 du Code pénal** Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
- **Article 226-18 du Code pénal** : Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
- **Article 226-21 du Code pénal** : Le fait, par toute personne détentrice d'informations nominatives à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative ou l'acte réglementaire autorisant le traitement automatisé, ou par la décision de la Commission nationale de l'informatique et des libertés autorisant un traitement automatisé ayant pour fin la recherche dans le domaine de la santé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
- **Article 226-22 du Code pénal** : Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
- **Article 323-1 du Code Pénal** : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 € d'amende.
- **Article 323-2 du Code Pénal** : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.
- **Article 323-3 du Code Pénal** : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.

- **Article 434-23 du Code Pénal** : Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.
- **Article 226-4-1 du Code Pénal** : Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.
- **Article 226-13 du Code Pénal** : La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende
- **Article 226-15 du Code Pénal** : Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 € d'amende.

3.2. *(Extraits)* Dispositions pénales du code de la propriété intellectuelle

- **Article L122-4 du Code la propriété intellectuelle** : « *Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque* ».

- **Article L335-2-1 du Code la propriété intellectuelle** : « *Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait :*
1° D'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés ;
2° D'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au 1° ».

- **Article L335-3 du Code la propriété intellectuelle** : « *Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.*

Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L.122-6.

Est également un délit de contrefaçon toute captation totale ou partielle d'une œuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique ».

Glossaire :

CNIL : Commission Nationale Informatique et Libertés - Créée en 1978, la CNIL est une autorité administrative indépendante qui exerce ses missions conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 20 juin 2018. Les dix-huit membres qui la composent sont pour la plupart élus par les assemblées ou les juridictions auxquelles ils appartiennent. La CNIL est investie d'une mission générale d'information des personnes des droits que leur reconnaît la loi Informatique et Libertés. La CNIL répond aux demandes des particuliers et des professionnels. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques

Charte : Les **chartes** sont des actes juridiques signés par plusieurs acteurs pour définir un objectif et parfois des moyens communs. Les chartes sont de natures variées :
Il existe des chartes :

- de qualité de produit ou de service, de respect des délais
- des chartes concernant les pratiques professionnelles des personnels

Déontologie : la déontologie professionnelle fait référence à l'ensemble de principes et règles éthiques qui gèrent et guident une activité professionnelle. Ces normes sont celles qui déterminent les devoirs minimums exigibles professionnels dans l'accomplissement de leur activité.

Devoir de réserve : Tout agent public doit faire preuve de réserve et de mesure dans l'expression écrite et orale de ses opinions personnelles. Cette obligation ne concerne pas le contenu des opinions (la liberté d'opinion est reconnue aux agents publics), mais leur mode d'expression.
L'obligation de réserve s'applique pendant et hors du temps de service.
Le manquement au devoir de réserve est apprécié par l'autorité hiérarchique au cas par cas.
Ce devoir s'applique plus ou moins rigoureusement selon :

- la place dans la hiérarchie, l'expression des hauts fonctionnaires étant jugée plus sévèrement,
- les circonstances dans lesquelles un agent s'est exprimé, un responsable syndical agissant dans le cadre de son mandat bénéficie de plus de liberté,
- la publicité donnée aux propos, si l'agent s'exprime dans un journal local ou dans un important média national,
- et les formes de l'expression, si l'agent a utilisé ou non des termes injurieux ou outranciers.

Cette obligation impose aussi aux agents publics d'éviter en toutes circonstances les comportements susceptibles de porter atteinte à la considération du service public par les usagers.

Discrétion professionnelle : Un agent public ne doit pas divulguer les informations relatives à l'activité, aux missions et au fonctionnement de son administration.

L'obligation de discrétion concerne les faits, informations ou documents non communicables aux usagers dont l'agent a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions.
Elle est particulièrement forte pour certaines catégories d'agents : les militaires ou les magistrats par exemple.
Cette obligation s'applique à l'égard des administrés mais aussi entre agents publics, à l'égard de collègues qui n'ont pas, du fait de leurs fonctions, à connaître les informations en cause.
Les responsables syndicaux restent soumis à cette obligation.
Cette obligation ne peut être levée que par décision expresse de l'autorité hiérarchique.

Données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable (ex. nom, no d'immatriculation, no de téléphone, adresse IP, adresse mail, photographie, date de naissance, commune de résidence, empreinte digitale...).

Données sensibles : Ce sont des données personnelles qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

DPD - DPO: Délégué à la Protection des Données en français ou Data Protection Officer en anglais. Il a pour mission d'informer et de conseiller son organisation, de contrôler l'application des textes légaux et des règles internes en matière de données personnelles (RGPD). Il fait office de point de contact entre son organisation et l'autorité de contrôle nationale : la CNIL.

DSI : Direction des Systèmes d'Information, responsable de l'ensemble des composants matériels et logiciels du système d'information, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre.

Fichier : Tout ensemble structuré de données à caractère personnel, quel que soit le support, papier ou numérique.

RENATER : Réseau national de télécommunications pour la technologie, l'enseignement et la recherche.
C'est un groupement d'intérêt public dont la création a été approuvée par un arrêté du 27 janvier 1993. Il s'agit d'un réseau informatique connectant plus de 1300 sites via des liaisons jusqu'à 10 Gbit/s (voir 100 Gbit/s entre 2 centres de calcul).
RENATER est connecté au réseau pan-européen GÉANT **(en)**. Il est également relié à Internet, en France via un point d'échange, le SFINX et dans le monde via 2 liaisons IP Transit de Paris et de Marseille.

RGPD : Le règlement **no 2016/679**, dit **Règlement Général sur la Protection des Données** (**RGPD**, ou encore **GDPR**, de l'anglais **General Data Protection Regulation**), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Après quatre années de négociations législatives, ce règlement a été définitivement adopté par le Parlement européen le 14 avril 2016. **Ses dispositions sont directement applicables** dans l'ensemble des **27 États membres de l'Union européenne** à compter du **25 mai 2018**.

RSSI : Responsable Sécurité des Systèmes d'Information, il est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise. Il est l'expert qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données.

Secret professionnel : Outre l'obligation de discrétion professionnelle, certains agents publics sont tenus, eu égard à leurs fonctions, au secret professionnel.
Cette obligation de secret s'applique aux informations relatives à la santé, au comportement, à la situation familiale d'une personne, etc., dont l'agent a connaissance dans le cadre de ses fonctions. Elle vise à protéger les intérêts matériels et moraux des particuliers.
Le secret professionnel peut être levé sur autorisation de la personne concernée par l'information.
La levée du secret professionnel est obligatoire pour assurer :

- la protection des personnes (révélation de maltraitances, par exemple),
- la préservation de la santé publique (révélation de maladies nécessitant une surveillance, par exemple),
- la préservation de l'ordre public (dénonciation de crimes ou de délits) et le bon déroulement des procédures de justice (témoignages en justice, par exemple).

En outre, les administrations doivent répondre aux demandes d'information de l'administration fiscale.
Le secret professionnel ne peut pas être invoqué pour refuser la communication de documents au Défenseur des droits. Exception : en matière de secret concernant la défense nationale, la sûreté de l'État ou la politique extérieure.
La révélation de secrets professionnels en dehors des cas autorisés est punie d'un an d'emprisonnement et de 15 000 € d'amende.

SI : Système d'Information, il peut être défini comme un ensemble de ressources (personnels, logiciels, processus, données, matériels, équipements informatiques et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo...) au sein d'une organisation.

SPAM : courriel indésirable ou pourriel, communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Traitement : Toute opération ou tout ensemble d'opérations portant sur ces données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Utilisateur/utilisatrice : Toute personne qui utilise les ressources informatiques et les moyens numériques de Réseau Canopé

VPN : Virtual Private Network – Réseau privé virtuel, tunnel d'accès et de transfert d'informations entre deux équipements informatiques chiffré de bout en bout.

Source : Wikipedia® (marque déposée de la Wikimedia Foundation, Inc.)